

ESERCITAZIONE EPICODE CREAZIONE REGOLA PFSENSE

- Per prima cosa sono andato ad abilitare una scheda di rete interna a Kali e l'ho assegnata a pfsense.
- Ho assegnato anche la rete interna di metasploitable a pfsense
- Per quanto riguarda pfsense ho impostato 3 schede di rete: una nat e due interne.

Ho assegnato a metasploitable il seguente ip statico:

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a1:ff:d9
          inet addr:192.168.32.100  Bcast:192.168.32.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea1:ffd9/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:101 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:27260 (26.6 KB)  TX bytes:11091 (10.8 KB)
          Base address:0xd020  Memory:f0200000-f0220000
```

IP di kali è il seguente:

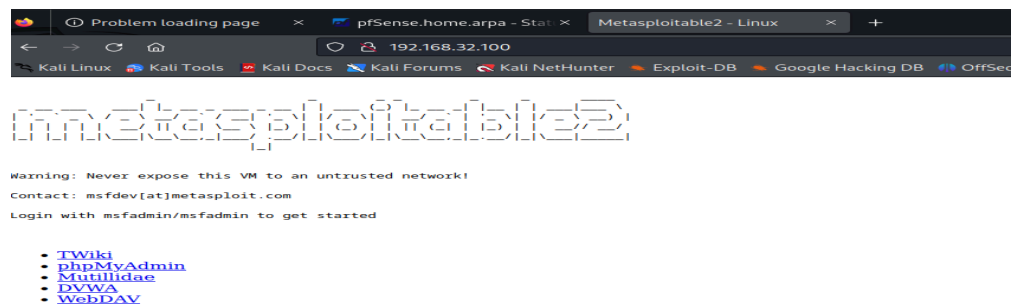
```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.50.100  netmask 255.255.255.0  broadcast 192.168.50.255
      inet6 fe80::a00:27ff:fe1b:d91d  prefixlen 64  scopeid 0x20<link>
      ether 08:00:27:1b:d9:1d  txqueuelen 1000  (Ethernet)
      RX packets 3000  bytes 932980 (911.1 KiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 2907  bytes 522924 (510.6 KiB)
      TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

A questo punto sono andato ad impostare le due schede LAN di pfsense. Alla prima ho inserito il gateway di kali "192.168.50.1" e alla seconda il gateway di Meta "192.168.32.1"

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)          -> em0          -> v4/DHCP4: 10.0.2.15/24
LAN (lan)           -> em1          -> v4: 192.168.50.1/24
OPT1 (opt1)        -> em2          -> v4: 192.168.32.1/24
```

A questo punto ho provato a pingare da kali e ad aprire tramite browser la pagina di meta. Queste a questo possono comunicare grazie a pfsense che instraderà i pacchetti da una macchina all'altra.



```

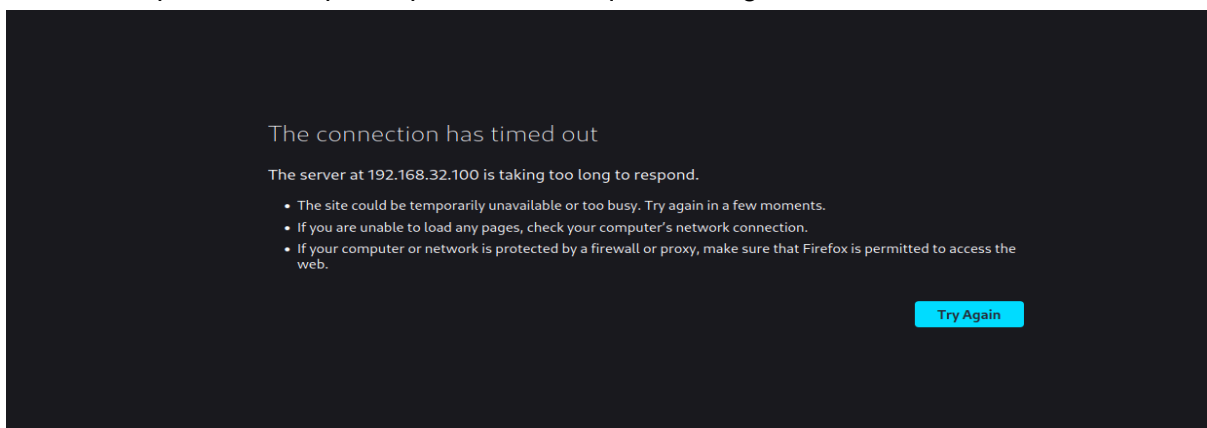
(kali@kali)-[~]
$ ping 192.168.32.100
PING 192.168.32.100 (192.168.32.100) 56(84) bytes of data.
64 bytes from 192.168.32.100: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from 192.168.32.100: icmp_seq=2 ttl=63 time=2.12 ms
64 bytes from 192.168.32.100: icmp_seq=3 ttl=63 time=2.79 ms
64 bytes from 192.168.32.100: icmp_seq=4 ttl=63 time=2.95 ms
^C
--- 192.168.32.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3486ms
rtt min/avg/max/mdev = 1.271/2.282/2.948/0.661 ms

```

Per impedire a Kali di accedere alla porta 80 di Metasploitable, creiamo una regola firewall dalla dashboard di pfsense andando su firewall/rules.

Action	Block		
	Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.		
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.		
Interface	LAN		
	Choose the interface from which packets must come to match this rule.		
Address Family	IPv4		
	Select the Internet Protocol version this rule applies to.		
Protocol	TCP		
	Choose which IP protocol this rule should match.		
Source			
	<input type="checkbox"/> Invert match	Address or Alias	192.168.50.100 /
Display Advanced			
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.			
Destination			
	<input type="checkbox"/> Invert match	Address or Alias	192.168.32.100 /
Destination Port Range	HTTP (80)	From Custom	To Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.			

Dopo aver salvato i cambiamenti sono andato a pingare di nuovo meta sulla porta 80 e ho notato che questa non è più disponibile e che quindi la regola creata ha funzionato.



```
(kali㉿kali)-[~]  
$ curl -v http://192.168.32.100 (opened 1000 (Ethernet))  
* Trying 192.168.32.100:80 ...  
* connect to 192.168.32.100 port 80 failed: Connection timed out  
* Failed to connect to 192.168.32.100 port 80 after 130923 ms: Couldn't connect to server  
* Closing connection 0  
curl: (28) Failed to connect to 192.168.32.100 port 80 after 130923 ms: Couldn't connect to server
```

MARGHERI LEONARDO